Global Journal of Computer Science and Technology: B
Cloud and Distributed
Volume 14 Issue 3 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

An Enhanced CBC Algorithm for Data Security in the Cloud

By Venkat Sampath Raja Gogineni & K. Raghava Rao
K L University, India

Abstract- Recent times, Storing data over the cloud has become more common for the reason that the data could be accessed globally .The data being stored on the cloud could involve confidential data, that needs security. The confidential data that is stored on the cloud through the database could be anything like username, email, password etc. This paper presents the idea/implementation of an Enhanced CBC algorithm on the cloud data. Through this cryptography technique the confidential data can be secured and authenticated.

Keywords: cloud security, encryption technique, modified CBC, database security, rail fence.

GJCST-B Classification : C.2.0

Strictly as per the compliance and regulations of:

An Enhanced CBC Algorithm for Data Security in the Cloud

Venkat Sampath Raja Gogineni [α] & K. Raghava Rao [σ]

Abstract- **Recent times, Storing data over the cloud has become more common for the reason that the data could be accessed globally .The data being stored on the cloud could involve confidential data, that needs security. The confidential data that is stored on the cloud through the database could be anything like username, email, password etc. This paper presents the idea/implementation of an Enhanced CBC algorithm on the cloud data. Through this cryptography technique the confidential data can be secured and authenticated.**

Keywords: cloud security, encryption technique, modified CBC, database security, rail fence.

I. Introduction

Cloud data, is the data that is to be stored over the network, the data that is corresponding to the client which could involve confidential details that needs to be secured. This data which is stored over the network is widely utilized for various useful aspects and needs to be sheltered from non-authenticated people.

When it comes to securing content of data, that could involve sensitive data such as usernames, passwords etc. There could be two types, one being restriction of access to the cloud and the other being the security of the data in the cloud. Though there are advancements in the firewall activities restricting the control of non-authenticated users, there are still the chances of hacking. So, securing data over the cloud is the other option , which involves the act of cryptography, with the best secured cryptographic algorithm the chances of securing data also gets impregnable.

II. Related Works

The Encryption algorithm that is used on the cloud data is stimulated using Verilog HDL and implemented on a web form that accepts client information to be stored over an external server (wamp server) through a servlet code consisting of an encryption algorithm, the values are thus stored in an encrypted form.

This Encryption algorithm which is a quite advancement or a modified CBC, is implemented on a string, where each character (8 bits) of a string is converted into binary format, on which the encryption algorithm mainly subsuming XOR and reverse operations is implemented. Unlike any other encryption algorithm in this one, the encryption key is generated from the text to be encrypted, which is also an 8-bit value. The first character binary value is XOR with the last character 8 bit binary value and thereby the result is XOR with the reversed binary bits of the middle character from the plain text to be encrypted, thereby generating a key of 8 bits. The key that is generated is again encrypted using rail fence technique and stored in the certain indexed position of the encrypted text.

Figure 1 : Register page

The above figure represents the html page that includes registration details of the client, the details are thus processed through the servlet code, which includes encryption algorithm, the text is encrypted and stored over the cloud (wamp server).

Author α σ: Dept. of Electronics and Computers. K L University, Guntur, AP. e-mails: sampath.gogineni@gmail.com, raghavarao@ kluniversity .in.

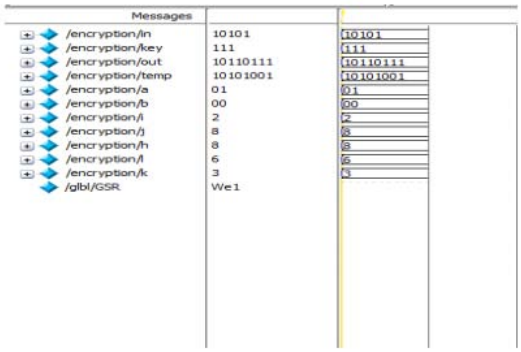

Figure 2 : Encryption Algorithm stimulation (CBC)

The algorithm is coded in Verilog HDL (Xilinx) and stimulated in Altera Modelsim. The stimulation represents the binary processing of a single character from the plain text in the encryption algorithm. With the represented input of 8 binary bits (temp variable in the above stimulation), through a generalized key of 8 bits (11111111), the encrypted binary output is calculated (out variable in the above stimulation), at the stage of implementation the binary output is converted into the character.

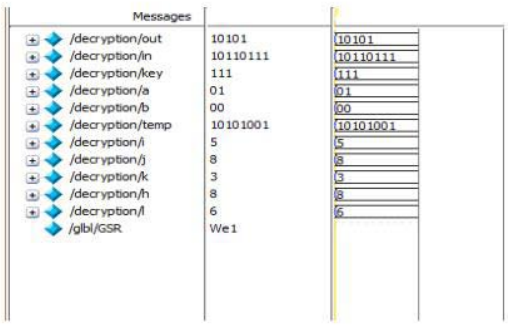

Figure 3 : Decryption Algorithm stimulation (CBC)

The above stimulation is for the decrypted 8 bit binary stature, where the encrypted output is given as the input (in variable in the above stimulation) through the same key used in the encryption, the plain text is thus obtained (temp in the above stimulation), Finally when it comes to implementation the binary output is converted in the form of a character.

The key that is used in this encryption algorithm is actually derived from the plain text, which is encrypted with the Rail fence encryption technique with the key value of 3 which is then added at a certain position in the encrypted text.

Figure 4 : Encryption Algorithm stimulation of key (Rail Fence)

The stimulation of Fig.4 represents the encrypted 8 bit binary stature of the key, with a series of different combination of rails. For the given input of 8 bits ("in" variable in the above stimulation), the encryption algorithm is applied and the encrypted output is calculated ("out" variable in the above stimulation). The 8 bit binary of the key is converted into a character and is embedded with the encrypted cipher text.

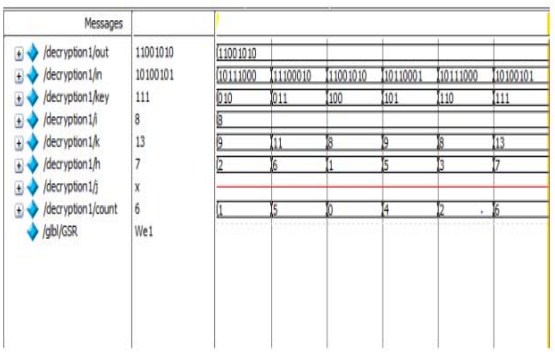

Figure 5 : Decryption Algorithm stimulation of key (Rail Fence)

The stimulation shown above represents the decryption of the key that is embedded at a certain position in the cipher text encrypted message, where the encrypted key output that is converted from string to binary is given as the input ("in" variable in the above stimulation) with the decryption of Rail fence algorithm original key is obtained ("out" in the above stimulation), To be implemented the 8 bit binary value is converted into a character.

III. Methodology

a) Cipher Blocking Chain (CBC)

CBC algorithm is the operation on the block of binary bits with a key. Each block of plain text is XOR

with the cipher block of previous one before encryption. Key is used to make the cipher blocks unique [1].

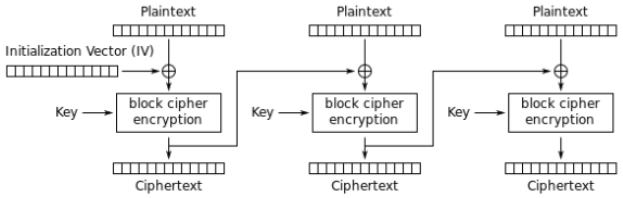

Figure 6 : CBC Encryption

Encryption technique in CBC is a serialized process, where the encryption undergoes process only if the previous block of message is encrypted.

Formula for Encryption Algorithm

$$C_i = E_K(P_i \oplus C_{i-1}), C_0 = IV$$

In this encryption algorithm each character is divided into 8 bit binary format, which is further divided into 4 blocks of two binary bits. The first block is reversed and XOR with the first block of key, the remaining blocks of data is XOR with the cipher of the first block, reversed, and then the result is stored and XOR with the key making the remaining 3 cipher blocks. Finally the 8 bit cipher represents single encrypted character. Similarly this is repeated on the remaining characters.

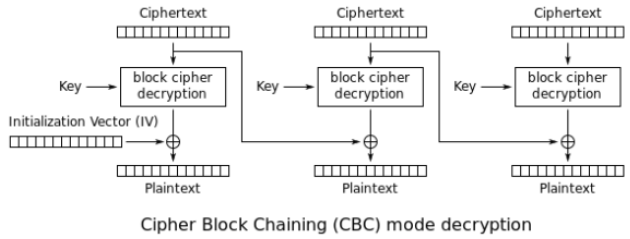

Figure 7 : CBC Decryption

Formula for Decryption Algorithm

$$P_i = D_K(C_i) \oplus C_{i-1}, C_0 = IV.$$

Decryption is the parallelized process,, that undergoes in a parallel fashion, Each block comprises of 2 binary bits. Altogether a total of 8 bits , with four blocks .The first block of the cipher text is XOR with the first block of the key, which is then reversed deriving the first block of the original message and for the remaining blocks the current block of the cipher is XOR with the key, which is then reversed and again XOR with cipher of the previous block, thereby making the original plain text of the remaining blocks , Which represents the plaintext of a single character and when repeated on the series of multiple characters the entire original string will be attained.

Clearly a confidential and secured key is required for this cryptography technique. For the key to be generated , in this method there is a specific process where the 8 bit binary number of the first character is XOR with the binary number of the last character , thereby the result of these two is XOR with the reverse of the middle character . The key is then formulated and it is encrypted using Rail fence technique, and stored in the specific index of the text that is encrypted.

b) Rail Fence

Rail fence technique is the diagonal representation of the elements present, and thereby appending the elements serially. The key represents the length of the diagonal.

For example,

Plain text: 101001110

Encrypted text: 100001111

No: of Rails (key):3

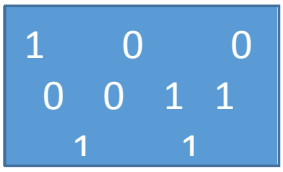

Figure 8 : Example of Rail Fence Technique

Clearly from the above figure, the length of the diagonal represents the no: of rails (key) and the plain text is diagonally arranged serially, and when the text is read in a serialized pattern, the encryption is done. The encrypted key of 8 bits is then embedded with the encrypted string (series of characters) at a certain position which is calculated as the (length of the string)/2 and then stored over the cloud.

Decryption is the reverse process of encryption, the key that is embedded at the (length of the string)/2 is identified and then decryption of Rail Fence technique is applied and finally the key for decryption is available.

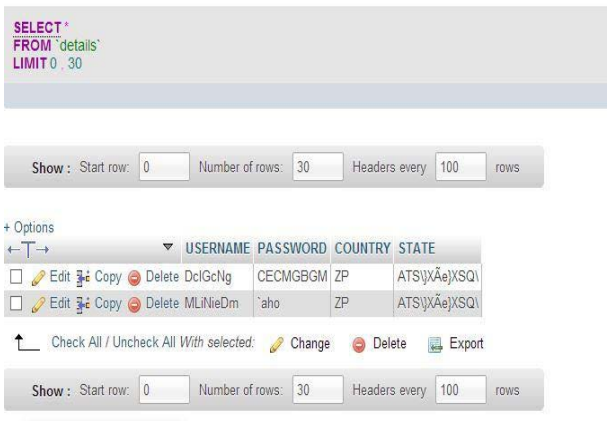

Figure 9 : Database in Encrypted form

After the client registers his information over the form a servlet which is embedded to the form will be provoked and the code of the algorithm stated written in java will be coded through the servlet.

Finally the encrypted text is stored over the cloud, rather than the plain text, that is clearly represented in the Fig 3. Similarly Decryption is the reverse process which is a parallelized one.

IV. Conclusion

The sensitive details of the user when registered will be encrypted using the encryption algorithm processed through the servlets and finally stored over the cloud, the key that is used in this encryption process is generated automatically from the plain text, while the original text is obtained by decryption (which is the reverse process of encryption).

V. Future Work

The user at this extant is restricted from the third party accessing information , while in the future users text files, images , videos etc. will be protected over the cloud network through the cryptography techniques so that the authenticated users could only access the information thereby restricting it to the third party users.

References Références Referencias

1. Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement BY Gulshan Kumar and Mritunjay Rai
2. Tony Durgadas jagyasi, Jagdish Pimple ,Security Enhancement in Cloud Computing Using Triple DES Encryption Algorithm
3. Volume 2 , No 1, January-March 2013 ISSN:2319-2720 “A Comparative study of counter mode with Cipher block chaining Message authentiacation code protocol(CCMP) and Temporal Key Integrity Protocol (TKIP): Wireless Security .
4. Milind Mathur and Ayush Kesarwani. “Comparison between DES, 3DES, RC2, Blowfish,AES”
5. Parallel Key Encryption for CBC and interleaved CBC by S. Ashok kumar ,K.Karuppasamy,Balaji Srinivasan,V. Balasubramanian.
6. Efficient Computing With Cloud. Issue 3, March 2013 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering.
7. http://en.wikipedia.org/wiki/Block_cipher_mode_of_operation.
8. “International Journal of Advanced Research in Computer Science and Software Engineering” by Ajit Singh, Aarti Nandal , Swati Malik.

.